DOC IT Security Evaluation Checklist: IT Security Officer Responsibilities

An IT Security Officer (ITSO) is a DOC employee responsible for implementing and monitoring an operating unit's IT security program. This checklist provides ITSOs with a self-assessment tool, and their supervisors with a performance evaluation to, to evaluate the level of compliance with ITSO duties as established by the

- *DOC IT Security Program Policy and Minimum Implementation Standards* (ITSPP),
- *DOC Remote Access Policy and Minimum Implementation Standards* (RASP), and
- *DOC Policy on Password Management* (PPM).

This is an assessment of (name/operating unit/office)**:**		
	Self Assessment	**Assessment Date:**
	Third Party Evaluation	**Assessor** (name/title/org.):

Status Codes: **1** = Not Started **2** = In Process **3** = In Place

Performance Levels:

1 ITSO has comprehensive IT security policies in place

2 ITSO has comprehensive IT security policies as well as detailed procedures in place

3 ITSO has comprehensive IT security policies and detailed procedures in place that are fully implemented for the operating unit's IT security program

4 ITSO has fully implemented and tested comprehensive IT security policies and detailed procedures in place

5 ITSO has fully implemented and tested comprehensive IT security policies and detailed procedures in place as part of a fully integrated IT security program

IT Security Officer (ITSO) Responsibilities		**DOC Policy References**	**Status**	**Performance Level**
1	Develop and maintain operating unit IT security policy, procedures, standards, and guidance consistent with Departmental and federal requirements.	ITSPP 2.1.8		
2	Ensure that all systems have IT security documentation in place, including:	ITSPP 2.1.8		
	(a) Qualitative risk assessments;	ITSPP 2.1.8, 3.1.2		
	(b) Current and effective IT security plans that conform to NIST SP 800-18;	ITSPP 2.1.8, 3.5.2		
	(c) Annual system self-assessments that conform to NIST SP 800-26 guidance;	ITSPP 3.2.1.2		
	(d) Current and tested contingency plans; and	ITSPP 3.9.2		
	(e) Current certification and accreditation packages.	ITSPP 3.4.1.4		
3	Conduct self-assessments of the operating unit's IT Security Program annually, including monitoring of system user compliance with these policies, as part of their periodic IT security self-assessment program or automated system evaluations.	ITSPP 2.1.8, RASP, PPM, and 3(a) – (c)		
	(a) Prepare program-level self-assessments annually using NIST SP 800-26 guidance;	ITSPP 3.2.1.2		
	(b) Prepare program-level corrective action plans/plans of action and milestones (POAMs) for weaknesses found; and	ITSPP 3.2.1.5		
	(c) Track program- and system-level POAMs to completion, and provide monthly status updates to the Department IT Security Manager.	ITSPP 3.2.1.6, 3.2.1.7		
4	Maintain the IT system inventory tracking and provide updated inventories to the DOC IT Security Program Manager semi-annually (March and September).	ITSPP 2.1.8, 3.2.4.1		
5	Establish a process to ensure that all users (including the ITSO) receive periodic IT security awareness material and copies of rules of behavior, and are trained to fulfill their IT security responsibilities. Ensure that IT security awareness and training programs address DOC policies.	ITSPP 2.0.1, RASP, PPM, and 5(a)-(b)		

	IT Security Officer (ITSO) Responsibilities	DOC Policy References	Status	Performance Level
	(a) Establish procedures for an IT security awareness and training program for all operating unit personnel, including specialized training as necessary for system administrators, ITSOs, procurement staff, etc.	ITSPP 3.13.5, RASP, PPM		
	(b) Participate in training to maintain ITSO knowledge, skills, and abilities.	ITSPP 3.13.9, 3.14.11		
6	Act as the operating unit's central point of contact for all incidents, develop incident handling procedures, and report all incidents to the DOC CIRT.	ITSPP 2.1.8, 3.14.6		
7	Provide risk management information to systems administrators and others.	ITSPP 2.1.8, 3.1.1		
8	Participate as a voting member of the DOC IT Security Coordinating Committee (ITSCC), participate in special committees under the ITSCC, and provide other support for the ITSCC as appropriate.	ITSPP 2.1.8, 2.2.1		
9	Coordinate with the DOC IT Security Program Manager and CIPM, as well as OSY and OIG as appropriate on IT security matters.	ITSPP 2.1.8, 4.0, RASP		
10	Establish a process to ensure access privileges are revoked in a timely manner when the requirement for access ceases (e.g., transfer, resignation, retirement, change of job description, etc.)	ITSPP 2.0.1, RASP, PPM		
11	Establish a process to periodically review, on a sample basis, the licensing of software within their organization. And, report any infringements to the operating unit CIO's office.	ITSPP 3.2.1.3		
12	Ensure that personnel security controls are addressed in operating unit IT security program policy and system security plans, including:	ITSPP 3.6.0.1 and 12(a)-(d)		
	(a) User administration;	ITSPP 3.6.1, RASP		
	(b) Rules of behavior/acceptable use policies;	ITSPP 3.6.2, RASP		
	(c) Segregation of duties; and	ITSPP 3.6.3		
	(d) Personnel termination and transfer.	ITSPP 3.6.4, RASP		
13	Ensure that all operating unit employees understand software copyright rules of behavior guidance.	ITSPP 3.10.4.1		
14	Establish a process to identify, track, and report on security patch management.	ITSPP 3.10.6.1		
15	Establish a Chain of Custody that documents (in writing) the name, title, office, and phone number of each individual having sequential possession of a system's hard drive, when it is removed due to compromise and the need for possible forensic examination of evidence for potential prosecution.	ITSPP 3.14.12		
16	Establish an optimal, cost-effective, configuration for network boundary devices that includes procedures and a schedule for periodic testing of incoming filtering protection.	ITSPP 3.16.3.2 and 3.16.3.5		
17	Ensure that cryptography is used for transmission of classified national security information, in accordance with the DOC Security Manual, Chapter 22	ITSPP 3.16.7.3		
18	Ensure that remote systems are monitored for compliance with DOC policies (as technically possible)	ITSPP 3.2.2.1, RASP		
19	Notify managers, supervisors, or COTRs to pursue appropriate disciplinary action and termination of remote user access privileges when users violate DOC policies.	RASP		
20	Ensure that the network warning banner communicates that there is no expectation of privacy in the authorized or unauthorized use of DOC IT systems	ITSPP 3.6.2.3		